Amendments to the Specification

On page 9, lines 3-19, please replace the existing paragraph with the following substitute paragraph:

A state consumption attack progresses as follows. A plurality of individual intranetworks ~~33,~~ 35 are interconnected via an internetwork 33 using conventional low- and high-bandwidth carriers interfaced via border routers 32 or similar devices. Other network topologies and configurations are feasible. An attacker 31 sends a stream of SYN request packets 37 with a fraudulent, that is, "spoofed," source address to a victim server 36 (step ①). The attacker 31 might also induce a plurality of servers 34 to send fraudulent SYN request packets 37 (step ②), such as through broadcast messaging. In turn, the victim server 36 allocates state (step ③) and sends SYN/ACK response packets to the system indicated in the source address of each SYN request packet 37. However, since the source addresses are spoofed, no ACK packets are returned and the state on the victim server 36 remains allocated until each request times out. If a sufficient number of SYN request packets 37 are sent in rapid succession, all available state in the victim server 36 will be allocated to service the fraudulent SYN request packets 37. Thus, no state will be available for valid requests and the service will be denied.

On page 11, lines 15-28, please replace the existing paragraph with the following substitute paragraph:

FIGURE 5 is a block diagram showing a system 70 for negotiating multi-path connections between a plurality of boundary controllers in a networked computing environment. For the purpose of illustration, the networked computing environment consists of three types of systems: a requesting client 71, a boundary controller (BC) 72 (or firewall or similar intermediary device), and a requested server 73. Each of these systems implement a TCP/IP network protocol stack which includes link 74, IP 75 and TCP 76, layers, such as described in W.R.

Stevens, "TCP/IP Illustrated," Vol. 1, Ch. 1 et seq., Addison-Wesley (1994), the disclosure of which is incorporated herein by reference. In addition, both the client 71 and server 73 implement client application 77 and server application ~~78~~ 79 layers. In the case of a DoS attack on the server 73, the client application 77 is a malicious application that bypasses ~~normal~~ the normal client TCP layer 76 and IP layer 75 to send spoofed segments in an attempt to consume the state of the TCP layer 76 of the server 73.

On page 11, line 29 through page 12, line 7, please replace the existing paragraph with the following substitute paragraph:

In the described embodiment, the boundary controller 72 intercedes between the client 71 and the server 73 to perform the three-way handshake sequence and terminate communication sessions, as further described below with reference to FIGURE 7. The boundary controller 72 functions as a pseudo server by exchanging client-boundary controller packets ~~79~~ 80 with the client 71 and boundary controller-server packets ~~80~~ 81 with the server 73. A client-boundary controller handshake sequence is first attempted by a validation module (not shown) of the boundary controller 72 and, if authenticated, a boundary controller-server handshake sequence is then performed.

On page 14, lines 11-21, please replace the existing paragraph with the following substitute paragraph:

FIGURE 7 is a timing diagram 90 showing, by way of example, the communication of connection parameters between a plurality of boundary controllers via an out-of-band communications channel. Briefly, a boundary controller 92 intercepts a session request from a requesting client 91 and only forwards the session request to a server 93 after checking the existence or validity of the requesting client 91 using a methodology such as described in the commonly assigned U.S. Patent No. 6,779,033, issued August 17, 2004, ~~Application, entitled "System And Method For Transacting A Validated~~

~~Application Session In A Networked Computing Environment," filed December 28, 2000, pending,~~ the disclosure of which is incorporated by reference. Non-existent or invalid session requests are discarded, thereby preventing state consumption leading up to a DoS attack.

On page 14, lines 27-30, please replace the existing paragraph with the following substitute paragraph:

The BC SYN-ACK packet 97 is addressed to the server at the source address specified in the TCP header of the client SYN packet ~~98~~ 96. If a valid requesting client 91 sent the client SYN packet 96, the requesting client 91 will respond to the server SYN-ACK packet 97 by sending a client ACK packet 98.

On page 15, lines 1-10, please replace the existing paragraph with the following substitute paragraph:

However, if the client SYN packet 96 was spoofed, that is, sent with a fraudulent source address, two outcomes exist. First, if the spoofed source address is not in use by another server, no responding client ACK packet ~~96~~ 98 will be generated and the original client SYN packet 96 will be ignored. Alternatively, if the spoofed source address is in use by another server but that server did not send the original client SYN packet 96, that server will send a client reset (RST) packet, as specified by the TCP. In either case, since the boundary controller 92 intercepted the spoofed client SYN packet 96 before reaching the server 93, no state is consumed or wasted, both on the server 93 and on the boundary controller 92.

On page 16, line 14 through page 17, line 2, please replace the existing paragraph with the following substitute paragraph:

FIGURE 8 is a timing diagram 110 showing, by way of example, the communication of connection parameters between a plurality of link layer

boundary controllers. A link layer boundary controller 112 intercepts a connection request sent as a client SYN packet 116 from a requesting client 111. The link layer boundary controller 112 indirectly shares the routing parameters of the client SYN packet 116 with the other link layer boundary controllers 113 using echo packets. The original client SYN packet 116 is encapsulated into an echo request packet 117 and forwarded to the requested server 115. The echo request packet 117 is identified as originating from the client 111 and addressed to the requested server 115. In reply, the server 115 sends an echo response packet 118 to the client 111. The link layer boundary controllers 112, 113 intercept the echo response packet 118 and store the connection parameters to complete the validation and authentication of the session request. Finally, another link layer boundary controller 113 generates a pseudo "server" SYN-ACK packet 119 to validate and authenticate the connection request using a methodology such as described in commonly assigned U.S. Patent Application serial number 09/655,515, filed August 31, 2000, pending, and U.S. Patent No. 6,772,334, issued August 3, 2004, ~~Application serial number 09/ 09/655,459, filed August 31, 2000, pending,~~ the disclosures of which are incorporated by reference.